

On Approximately Symmetric Informationally Complete Positive Operator-Valued Measures and Related Systems of Quantum States

ANDREAS KLAPPENECKER

Department of Computer Science

Texas A&M University

College Station, TX, 77843–3112, USA

`klappi@cs.tamu.edu`

MARTIN RÖTTELER

NEC Laboratories America, Inc.

Princeton, NJ 08540, U.S.A.

`mroetteler@nec-labs.com`

IGOR E. SHPARLINSKI

Department of Computing

Macquarie University,

Sydney, NSW 2109, Australia

`igor@ics.mq.edu.au`

ARNE WINTERHOF

Johann Radon Institute for

Computational and Applied Mathematics

Austrian Academy of Sciences

Altenbergerstr. 69, 4040 Linz, Austria

`arne.winterhof@oeaw.ac.at`

February 1, 2008

Abstract

We address the problem of constructing positive operator-valued measures (POVMs) in finite dimension n consisting of n^2 operators of rank one which have an inner product close to uniform. This is motivated by the related question of constructing symmetric informationally complete POVMs (SIC-POVMs) for which the inner products are perfectly uniform. However, SIC-POVMs are notoriously hard to construct and despite some success of constructing them numerically, there is no analytic construction known. We present two constructions of approximate versions of SIC-POVMs, where a small deviation from uniformity of the inner products is allowed. The first construction is based on selecting vectors from a maximal collection of mutually unbiased bases and works whenever the dimension of the system is a prime power. The second construction is based on perturbing the matrix elements of a subset of mutually unbiased bases.

Moreover, we construct vector systems in \mathbb{C}^n which are almost orthogonal and which might turn out to be useful for quantum computation. Our constructions are based on results of analytic number theory.

1 Introduction

1.1 Background

A basic question in quantum mechanics is how to obtain information about the state of a given physical system by using suitable measurements. Even in case many identically prepared copies of the system are available, it is a nontrivial task to devise a measurement procedure which uniquely identifies the given quantum state from the statistical data produced by the measurements. Note that this holds true even in case the complete statistics, that is, the probabilities for the different measurement outcomes, is known.

We next describe the possible measurements of the quantum system in more detail and first remark that all systems considered in this paper are of finite dimension n . If the state of the quantum system is given by an $n \times n$ density matrix, then the complete measurement statistics of one fixed *von Neumann measurement* is not sufficient to reconstruct the state. Indeed, this follows from the fact that the statistics of a fixed von Neumann measurement

determines at most $n - 1$ real parameters (specified by the probabilities of the measurement outcomes), whereas a general density matrix is determined by $n^2 - 1$ free real parameters.

In fact it is possible to perform a more general measurement procedure on a quantum system, namely a *positive operator-valued measure*, or POVM for short, see [33, 34]. A POVM is described by a collection of positive operators $E_i \geq 0$, called POVM elements, that partition the identity, that is, $\sum_i E_i = I_n$. If the state of the quantum system is given by the density matrix ρ , then the probability p_i to observe outcome i in the POVM is given by the Born rule

$$p_i = \text{tr}(\rho E_i), \quad (1)$$

where $\text{tr}(A)$ denotes the trace of a complex matrix A . The task is to devise a POVM with operators E_i such that the state ρ is uniquely specified by the probabilities p_i in (1). The POVM is then called *informationally complete*, or simply an IC-POVM, and they appear to have been first studied in [38]. A particularly interesting question is whether a POVM exists on \mathbb{C}^n that consists of n^2 POVM elements E_i of rank one. Counting the number of parameters determined by the measurement, we see that n^2 is indeed the minimal possible number of such POVM elements. In this case E_i is a subnormalized projector, that is, $E_i = \Pi_i/n$ for projectors $\Pi_i = |\psi_i\rangle\langle\psi_i|$ corresponding to some vectors $|\psi_i\rangle$ in \mathbb{C}^n . In [12] it has been shown that IC-POVMs exist in all dimensions and in [15] a method has been given how to construct IC-POVMs by taking a fixed fiducial start vector $|\psi\rangle$ and taking the orbit of this vector under a (projective) group operation.

As an example of this type, consider the normalized states $|\psi_1\rangle, \dots, |\psi_4\rangle$ defined as follows:

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{3} \begin{pmatrix} 1 \\ 2+2i \end{pmatrix}, & |\psi_2\rangle &= \frac{1}{3} \begin{pmatrix} 2+2i \\ 1 \end{pmatrix}, \\ |\psi_3\rangle &= \frac{1}{3} \begin{pmatrix} 1 \\ -2-2i \end{pmatrix}, & |\psi_4\rangle &= \frac{1}{3} \begin{pmatrix} 2+2i \\ -1 \end{pmatrix}. \end{aligned}$$

Then the rank one operators defined by $E_i = 1/2 |\psi_i\rangle\langle\psi_i|$ are given by

$$\begin{aligned} E_1 &= \frac{1}{18} \begin{pmatrix} 1 & 2+2i \\ 2-2i & 8 \end{pmatrix}, & E_2 &= \frac{1}{18} \begin{pmatrix} 8 & 2-2i \\ 2+2i & 1 \end{pmatrix}, \\ E_3 &= \frac{1}{18} \begin{pmatrix} 1 & -2-2i \\ -2+2i & 8 \end{pmatrix}, & E_4 &= \frac{1}{18} \begin{pmatrix} 8 & -2+2i \\ -2-2i & 1 \end{pmatrix}, \end{aligned}$$

and it can be verified easily that $E_1 + E_2 + E_3 + E_4 = I_4$ is the identity matrix and that the matrices E_1, E_2, E_3, E_4 are linearly independent. For the possible inner products between two POVM elements E_i and E_j where $i \neq j$ we obtain that $\text{tr}(E_i E_j) \in \{4/81, 49/324\}$.

Our goal is to find IC-POVMs on \mathbb{C}^n such that $n^2 \text{tr}(E_i E_j)$ is “small” for distinct POVM elements $E_i = |\psi_i\rangle\langle\psi_i|/n$ and $E_j = |\psi_j\rangle\langle\psi_j|/n$. In Section 1.3 we make precise what we mean by the inner products being small and briefly summarize previous work on the problem.

1.2 Notation

We use the Landau notation to compare the asymptotics of two functions $f, g : \mathbb{N} \rightarrow \mathbb{C}$. We recall that $f(n) = o(g(n))$ means $\lim_{n \rightarrow \infty} f(n)/g(n) = 0$. Furthermore, $f(n) = O(g(n))$ means that there exists a constant $c > 0$, such that $|f(n)| \leq cg(n)$ for all $n \geq 1$. Throughout the paper, the implied constants in the symbols ‘ o ’ and ‘ O ’ may occasionally, where obvious, depend on an integer parameter d and a small real parameter $\varepsilon > 0$, and are absolute otherwise.

For an integer $n \geq 1$ we denote by \mathbb{C}^n the n -dimensional vector space over the complex numbers \mathbb{C} . For two vectors $|\psi\rangle = (a_1, \dots, a_n) \in \mathbb{C}^n$ and $|\varphi\rangle = (b_1, \dots, b_n) \in \mathbb{C}^n$, we use

$$\langle\psi|\varphi\rangle = \sum_{i=1}^n \bar{a}_i b_i$$

to denote their inner product. We also define $\delta_{i,j} = 1$ if $i = j$ and 0 otherwise. We denote the identity matrix of size $n \times n$ by I_n , the all-ones matrix of size n by $J_n = [1]_{i,j=1}^n$. We use $\text{diag}(a_1, \dots, a_n)$ to denote the $n \times n$ diagonal matrix which has a_1, \dots, a_n on the main diagonal. For matrices A and B , we use $A \oplus B$ to denote their block-diagonal direct sum.

For a real z and an integer m we use the notation $\mathbf{e}_m(z) = \exp(2\pi\iota z/m)$, where $\iota = \sqrt{-1}$.

We use \mathbb{F}_q to denote the finite field of q elements, and we also assume that for a prime p , the field \mathbb{F}_p is represented by the set $\{0, \dots, p-1\}$.

As we have mentioned, we use $\text{tr}(A)$ to denote the trace of a complex matrix A . On the other hand, for an element $a \in \mathbb{F}_q$ we use $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)$ to

denote its trace in the prime subfield \mathbb{F}_p of \mathbb{F}_q , see [31]. That is, if $q = p^m$ for a prime m , then

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a) = \sum_{j=0}^{m-1} a^{p^j}.$$

1.3 Previously Known Results

A particularly appealing case of IC-POVMs arises when furthermore all of the inner products of the vectors $|\psi_i\rangle$ are small. An extremal case in this sense arises when we are given a system of n^2 normalized vectors $\{|\psi_i\rangle : i = 1, \dots, n^2\}$ in \mathbb{C}^n for which

$$|\langle\psi_i|\psi_j\rangle|^2 = \frac{1}{n+1}, \quad 1 \leq i < j \leq n^2. \quad (2)$$

Indeed, for any system of k vectors $|\psi_1\rangle, \dots, |\psi_k\rangle$ in \mathbb{C}^n for which the absolute values of pairwise inner products are constant $|\langle\psi_i|\psi_j\rangle|^2 = \alpha$, where $\alpha \in \mathbb{R}$ (for $1 \leq i < j \leq k$) the so-called special bound holds [23] which says that $k \leq \frac{n(1-\alpha)}{1-n\alpha}$. Specializing $\alpha = 1/(n+1)$ we obtain that n^2 is the largest possible number of vectors satisfying (2).

A system of vectors as in (2), respectively the corresponding POVMs, are called *symmetric informationally complete POVMs*, or SIC-POVMs for short. They have several very desirable properties, see [12] for a discussion in the context of the quantum de Finetti theorem and more generally in their Bayesian approach to quantum mechanics and its interpretation [11]. Furthermore, see [18, 19] for their role in establishing the quantumness of a Hilbert space and the related question about optimal intercept-resend eavesdropping attacks on quantum cryptographic schemes. Explicit analytical constructions of sets satisfying (2) have been given for dimensions $n = 2, 3, 4, 5$ in [50, Section 3.4] and [41], for dimension $n = 6$ in [20], for dimensions $n = 7, 19$ in [1] and for dimension $n = 8$ see [24]. While it has been conjectured that SIC-POVMs exist in all dimensions [50, Section 3.4] or [41] and numerical evidence exists for dimensions up to 45, see [41], it is a difficult task to explicitly construct systems of vectors which satisfy (2). There are no known infinite families of SIC-POVMs and in fact it is not even clear if there are SIC-POVMs for infinitely many n .

1.4 Our Results

In the first part (Section 2) of this paper we relax condition (2) on the inner products slightly and allow that

$$|\langle \psi_i | \psi_j \rangle|^2 \leq \frac{1 + o(1)}{n}, \quad 1 \leq i < j \leq n^2. \quad (3)$$

The purpose of the first part of this paper is to show that infinite families of systems of n^2 normalized vectors which satisfy (3) and give rise to IC-POVMs exist. We call the rank one projectors obtained from such systems of vectors *approximately symmetric informationally complete POVMs*, or ASIC-POVMs for short. Here we show that when $n = p^r$ is a power of a prime p , ASIC-POVMs can be constructed.

In the second part (Section 3) of the paper we explore properties of other approximately symmetric vector systems where we do not require the properties of completeness and informational completeness but require the property of approximate symmetry. We also relax (3) further by allowing that the inner products be bounded from above by $|\langle \psi_i | \psi_j \rangle| \leq (2 + o(1))/\sqrt{n}$ and by dropping the requirement that the vectors give rise to a POVM. This additional freedom then allows us to construct bases in all dimensions n . Besides their general mathematical interest in constructing such vector systems they might be useful in quantum cryptographic scenarios which generalize the BB84 setting [7], such as the protocols described in [8, 39, 40]. See also [14] for an analysis of general schemes for quantum key distribution where the sender uses arbitrary quantum states and the receiver's measurement is replaced by a POVM.

Besides approximations to SIC-POVMs we also consider approximations to *mutually unbiased bases* (MUBs). Since we also need MUBs for our construction of ASIC-POVMs we briefly recall their definition. A maximal set of MUBs is given by a set of $n^2 + n$ vectors in \mathbb{C}^n which are the elements of $n + 1$ orthonormal bases $\mathcal{B}_k = \{|\psi_{k,1}\rangle, \dots, |\psi_{k,n}\rangle\}$ of \mathbb{C}^n where $k = 0, \dots, n$. Hence,

$$\langle \psi_{k,i} | \psi_{k,j} \rangle = \delta_{i,j}, \quad (4)$$

and the defining property is the mutual unbiasedness, given by

$$|\langle \psi_{k,i} | \psi_{\ell,j} \rangle| = \frac{1}{\sqrt{n}} \quad (5)$$

for $0 \leq k, \ell \leq n$, $k \neq \ell$, and $1 \leq i, j \leq n$. Starting from [26, 42, 49] an extensive growing body of research explores MUBs and their constructions, see [2, 4, 6, 13, 17, 21, 27, 36, 37, 48] and references therein. However, so far maximally sets of $n + 1$ MUBs in dimension n are only known to exist in any dimension $n = p^r$ which is a power of a prime $p \geq 3$, see [27] for an overview and some of such constructions. The main construction is based on Gaussian sums and in the case of prime $n = p$ can be described as

$$|\psi_{k,j}\rangle = \frac{1}{\sqrt{p}} \left(\mathbf{e}_p(ku^2 + ju) \right)_{u=1}^p, \quad 1 \leq k, j \leq p,$$

and also \mathcal{B}_0 being a standard orthonormal basis, that is, $|\psi_{0,j}\rangle = (\delta_{j,u})_{u=1}^p$.

One can use additive characters over an arbitrary finite field to extend this construction to an arbitrary prime power $n = p^r$. However the condition that $n = p^r$ is a prime power is still somewhat too restrictive and unnatural for quantum computation. So a natural question arises whether MUBs exist for every positive integer n . In the second part we consider vector systems where we relax the conditions (3) and (5). We use exponential sums to construct vector systems for any dimension n which

- satisfy (4) but instead of (5) all other inner products are $O(n^{-1/4})$;
- is normalized but instead of (2) all other inner products are at most $(2 + o(1))n^{-1/2}$.

We call vector systems of $n^2 + n$ vectors in \mathbb{C}^n which satisfy (4), and instead of (5) the condition

$$|\langle \psi_i | \psi_j \rangle|^2 \leq \frac{1 + o(1)}{n}, \quad 1 \leq i < j \leq n^2 + n$$

approximately mutually unbiased bases, or AMUBs for short.

We also construct some vector systems using multiplicative and mixed character sums, which

- satisfy (4) and assuming some natural and widely believed conjecture on the distribution of primes in arithmetic progressions all other inner products are $O(n^{-1/2} \log n)$;

- in the special case of $n = p - 1$ where p is a prime, form AMUBs.

Interestingly, our arguments use both the classical bound of Weyl [47] (see also [25, 43]) as well as the more recent, but no less celebrated, bounds of Weil [45] (see also [30, 31, 46]). Besides exponential sum techniques we also use some recent results about the gaps between prime numbers from [3]. We conclude with some conjectures and open questions concerning our constructions in Section 4.

2 Constructing ASIC-POVMs

2.1 Preliminaries

We begin by giving a definition of the vectors and associated rank one operators we are interested in.

Definition 1 (ASIC-POVMs). *Suppose that n is a positive integer. Let $\mathcal{A} = \{|\psi_i\rangle : i = 1, \dots, n^2\}$ be a set of vectors in \mathbb{C}^n . Let $\mathcal{E} = \{E_i = |\psi_i\rangle\langle\psi_i|/n : i = 1, \dots, n^2\}$ be the corresponding set of subnormalized projection operators. If \mathcal{E} satisfies the conditions*

- (i) $\sum_{i=1}^{n^2} E_i = I_n$ (completeness/POVM condition);
- (ii) the matrices E_i are linearly independent as elements of $\mathbb{C}^{n \times n}$ (informational completeness);
- (iii) $|\langle\psi_i|\psi_j\rangle|^2 = n^2 \text{tr}(E_i E_j) \leq (1 + o(1))n^{-1}$ for $1 \leq i < j \leq n^2$ (approximate symmetry);

then we call \mathcal{E} an approximately symmetric informationally complete POVM, or ASIC-POVM for short.

We remark, that in fact, sometimes we also refer to the corresponding set \mathcal{A} as an ASIC-POVM.

In the subsequent sections, we present two different constructions that give rise to infinite families of ASIC-POVMs. The first construction is based on the observation that a set of $n + 1$ mutually unbiased bases in \mathbb{C}^n gives

rise to an IC-POVM, cf. [26, 49]. However, this IC-POVM consists of $n^2 + n$ rank-one operators; thus, it is an overcomplete generating set of the vector space of all $n \times n$ matrices. In our first construction in Section 2.3 we show how to select n^2 projectors that allow us to derive an ASIC-POVM. The second construction in Section 2.4 starts from all vectors contained in n of the $n + 1$ MUBs. We show that by slightly perturbing the components of these vectors it is possible to obtain an ASIC-POVM.

2.2 POVMs and Frames

Suppose that $\mathcal{A} = \{|\psi_i\rangle \in \mathbb{C}^n : 1 \leq i \leq n^2\}$ is a system of n^2 vectors of unit norm, such that \mathcal{A} spans \mathbb{C}^n and the associated subnormalized projectors $E_i = |\psi_i\rangle\langle\psi_i|/n$ satisfy $n^2\text{tr}(E_i E_j) = (1 + o(1))n^{-1}$ whenever $i \neq j$.

We would like to have that the subnormalized projectors E_i form a POVM, but, unfortunately, the completeness relation $\sum_{i=1}^{n^2} E_i = I_n$ is in general not satisfied. However, there is a way to fix this using a technique described in [12]: Define a positive semidefinite hermitian operator G by

$$G = \sum_{i=1}^{n^2} E_i.$$

Since \mathcal{A} spans \mathbb{C}^n , the inequality $\langle\varphi|G|\varphi\rangle = \sum_i |\langle\psi_i|\varphi\rangle|^2 > 0$ holds for any nonzero vector $|\varphi\rangle$ in \mathbb{C}^n , so G is even positive definite. It follows that G^{-1} exists and is positive definite, and we can form the uniquely determined positive definite square-root $G^{-1/2}$. The n^2 rank-one operators

$$\mathcal{E} = \{F_i = G^{-1/2} E_i G^{-1/2} : 1 \leq i \leq n^2\}$$

form a POVM, since $\sum_i F_i = G^{-1/2} G G^{-1/2} = I_n$.

Clearly, if the operators E_i are linearly independent, then so are the operators F_i . Therefore, the procedure preserves information-completeness.

In general, if we switch from the rank-one operators E_i to the rank-one operators F_i , then $\text{tr}(F_i F_j) \leq (1 + o(1))/n^3$ might not hold for some $i \neq j$. However, if G^{-1} is close to the identity matrix, then approximate symmetry is preserved as well.

We now mention some connections between POVMs and the theory of frames [5, 9, 16].

Definition 2 (Frames). A set $\mathcal{F} = \{|\psi_i\rangle : 1 \leq i \leq N\}$ of vectors in \mathbb{C}^n is called a frame if there exist real numbers a and b , with $0 < a \leq b$, such that

$$a\langle\varphi|\varphi\rangle \leq \sum_{i=1}^N |\langle\varphi|\psi_i\rangle|^2 \leq b\langle\varphi|\varphi\rangle$$

holds for all $|\varphi\rangle \in \mathbb{C}^n$.

If $a = b$, then the frame is called a tight frame, and if $a = b = 1$ then the frame is called a Parseval frame.

We can associate with the frame \mathcal{F} its frame operator $G = \sum_{k=1}^N |\psi_k\rangle\langle\psi_k|$. If we are given a frame \mathcal{F} with frame operator G , then

$$\mathcal{G} = \{G^{-1/2} |v\rangle : |v\rangle \in \mathcal{F}\}$$

is a Parseval frame, see [10, Theorem 4.2]. The projectors associated with \mathcal{G} form a POVM, since $\sum_{v \in \mathcal{F}} G^{-1/2} |v\rangle\langle v| G^{-1/2} = G^{-1/2} G G^{-1/2} = I$ holds.

If we have a Parseval frame \mathcal{G} in \mathbb{C}^n with n^2 elements such that the associated projection operators are linearly independent and the frame elements satisfy the approximate symmetry (3), then the projectors corresponding to the frame \mathcal{G} form an ASIC-POVM.

2.3 Construction I: Pruning MUBs

The first construction of ASIC-POVMs is based on the idea to select a suitable collection of n^2 vectors from a set of $n^2 + n$ vectors that form a maximal set of $n + 1$ mutually unbiased bases of \mathbb{C}^n . Our goal is to choose n^2 vectors such that the corresponding projection operators are linearly independent. We recall a known fact that belongs to the folklore of mutually unbiased bases; it is implicitly contained in [26, 49], and more explicitly in [22], and our proof is based on the latter.

Lemma 3. Suppose that $\mathcal{B}_a = \{v_{a,b} : 0 \leq b < n\}$, with $0 \leq a \leq n$, are $n + 1$ mutually unbiased bases of \mathbb{C}^n , and let

$$\mathcal{P} = \{|v_{a,b}\rangle\langle v_{a,b}| : 0 \leq a \leq n, 0 \leq b < n\}$$

denote the associated set of $n^2 + n$ projectors. The n^2 projection operators in $\mathcal{P}^* = \{|v_{a,b}\rangle\langle v_{a,b}| : (a,b) = (0,0) \text{ or } b \neq 0\} \subset \mathcal{P}$ are linearly independent.

Proof. First, suppose that a linear relation

$$\sum_{a=0}^n \sum_{b=0}^{n-1} \gamma_{a,b} |v_{a,b}\rangle \langle v_{a,b}| = 0 \quad (6)$$

holds for some $\gamma_{a,b} \in \mathbb{C}$. We are going to show that this has some rather strong consequences for the coefficients $\gamma_{a,b}$. If we apply the projection operators from \mathcal{P} and take the trace, then we obtain a linear system of equations $A\mathbf{g} = 0$, where

$$A = [\text{tr}(|v_{a,b}\rangle \langle v_{a,b}| |v_{c,d}\rangle \langle v_{c,d}|)]_{(a,b),(c,d)}$$

and $\mathbf{g} = (\gamma_{a,b})$ is a column vector. The matrix A is block-circulant,

$$A = \begin{pmatrix} I_n & \frac{1}{n}J_n & \cdots & \frac{1}{n}J_n & \frac{1}{n}J_n \\ \frac{1}{n}J_n & I_n & \cdots & \frac{1}{n}J_n & \frac{1}{n}J_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{1}{n}J_n & \frac{1}{n}J_n & \cdots & \frac{1}{n}J_n & I_n \end{pmatrix},$$

with $n \times n$ identity matrices in the diagonal blocks, and multiples of the $n \times n$ all-one matrix in the off-diagonal blocks.

If we subtract two equations in $A\mathbf{g} = 0$ that belong to the same block row, then we find that $\gamma_{a,b} = \gamma_{a,d}$ holds for all $0 \leq b, d < n$ and all indices a . Therefore, the coefficients $\gamma_{a,b}$ do not depend on the value of b .

Finally, suppose that the left hand side of (6) consists of a linear combination of projectors belonging to the set \mathcal{P}^* , meaning that the coefficients $\gamma_{a,b} = 0$ when $a \neq 0$ and $b = 0$. It follows that $\gamma_{a,b} = 0$ holds whenever $a \neq 0$, since $\gamma_{a,b} = \gamma_{a,0}$ by our previous observation. Therefore, the left hand side of (6) reduces to

$$\sum_{b=0}^{n-1} \gamma_{0,b} |v_{0,b}\rangle \langle v_{0,b}| = \sum_{b=0}^{n-1} \gamma_{0,0} |v_{0,b}\rangle \langle v_{0,b}| = 0.$$

Thus, we must have $\gamma_{0,0} = 0$. Therefore, we can conclude that the projectors in \mathcal{P}^* are linearly independent, as claimed. \square

We also recall the basic construction of MUBs in prime power dimension; see, for instance, [27, 49].

Lemma 4. *Let q be a power of a prime $p \geq 3$. Define*

$$|\psi_{a,b}\rangle = q^{-1/2} \left(\mathbf{e}_p \left(\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax^2 + bx) \right) \right)_{x \in \mathbb{F}_q} \in \mathbb{C}^q.$$

Then the standard basis \mathcal{B}_0 together with the bases $\mathcal{B}_a = \{|\psi_{a,b}\rangle : b \in \mathbb{F}_q\}$, $a \in \mathbb{F}_q$, form a set of $q+1$ mutually unbiased bases of \mathbb{C}^q .

Our first construction of ASIC-POVMs is given in the next theorem.

Theorem 5. *Let q be a power of a prime $p \geq 3$. Let*

$$|\psi_{a,b}\rangle = q^{-1/2} \left(\mathbf{e}_p \left(\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax^2 + bx) \right) \right)_{x \in \mathbb{F}_q} \in \mathbb{C}^q$$

for all $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q^\times$ and $|\psi_{a,0}\rangle = (\delta_{a,x})_{x \in \mathbb{F}_q}$ for all $a \in \mathbb{F}_q$. We define $E_{a,b} = |\psi_{a,b}\rangle \langle \psi_{a,b}| / q$ and

$$G = \sum_{a \in \mathbb{F}_q} \sum_{b \in \mathbb{F}_q} E_{a,b}.$$

Then the set $\{F_{a,b} : a, b \in \mathbb{F}_q\}$, with $F_{a,b} = G^{-1/2} E_{a,b} G^{-1/2}$, is an ASIC-POVM.

Proof. The linear independence of the operators $E_{a,b}$ follows from Lemma 3. It remains to show that the matrix G^{-1} is close to the identity and that $F_{a,b} = G^{-1/2} |\psi_{a,b}\rangle \langle \psi_{a,b}| G^{-1/2}$ indeed forms an ASIC-POVM. First, we explicitly compute the frame operator G . We have

$$\begin{aligned} G &= \frac{1}{q} \sum_{(a,b) \in \mathbb{F}_q \times \mathbb{F}_q^\times} |\psi_{a,b}\rangle \langle \psi_{a,b}| + \frac{1}{q} I_q \\ &= \frac{1}{q^2} \left(\sum_{x,y,a,b \in \mathbb{F}_q} \mathbf{e}_p \left(\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a(x^2 - y^2) + b(x - y)) \right) |x\rangle \langle y| \right. \\ &\quad \left. - \sum_{x,y,a \in \mathbb{F}_q} \mathbf{e}_p \left(\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a(x^2 - y^2)) \right) |x\rangle \langle y| \right) + \frac{1}{q} I_q. \end{aligned}$$

We notice that $\langle x | G | x \rangle = 1$ for $x \in \mathbb{F}_q$, $\langle x | G | -x \rangle = -1/q$ for $x \in \mathbb{F}_q^\times$, and $\langle x | G | y \rangle = 0$ for $x, y \in \mathbb{F}_q$ with $x \neq \pm y$. Therefore, we can express the operator G in the form

$$G = I_q - \frac{1}{q} Q + \frac{1}{q} |0\rangle \langle 0|, \quad \text{where} \quad Q = \sum_{x \in \mathbb{F}_q} |x\rangle \langle -x|.$$

Using the structure of G , it follows that the inverse is given by

$$G^{-1} = \left(1 + \frac{1}{q^2 - 1}\right) I_q + \frac{q}{q^2 - 1} Q - \frac{1}{q - 1} |0\rangle \langle 0|.$$

Observe that the set of vectors $\{|\psi_{a,b}\rangle : (a,b) \in \mathbb{F}_q \times \mathbb{F}_q^\times\}$ is invariant under Q , since $Q|\psi_{a,b}\rangle = |\psi_{a,-b}\rangle$. Recall that by Lemma 4 the bounds

$$|\langle \psi_{a,b} | \psi_{c,d} \rangle| \leq q^{-1/2}$$

hold, whenever $(a,b) \neq (c,d)$. Defining $|\tilde{\psi}_{a,b}\rangle = G^{-1/2} |\psi_{a,b}\rangle$ we get

$$F_{a,b} = G^{-1/2} E_{a,b} G^{-1/2} = |\tilde{\psi}_{a,b}\rangle \langle \tilde{\psi}_{a,b}| / q$$

and obtain that

$$\begin{aligned} q^2 \text{tr}(F_{a,b} F_{c,d}) &= |\langle \tilde{\psi}_{a,b} | \tilde{\psi}_{c,d} \rangle|^2 = |\langle \psi_{a,b} | G^{-1} | \psi_{c,d} \rangle|^2 \\ &\leq \left| \left(1 + \frac{1}{q^2 - 1}\right) \langle \psi_{a,b} | \psi_{c,d} \rangle \right|^2 \\ &\quad + \left| \left(\frac{q}{q^2 - 1}\right) \langle \psi_{a,b} | \psi_{c,-d} \rangle \right|^2 + \left(\frac{1}{q(q-1)}\right)^2 \\ &\leq \frac{1}{q} \left(1 + \frac{1}{q^2 - 1}\right)^2 + \frac{1}{q} \left(\frac{q}{q^2 - 1}\right)^2 + \left(\frac{1}{q(q-1)}\right)^2 \\ &= \frac{1 + o(1)}{q}. \end{aligned}$$

This shows that the rank-one operators $F_{a,b}$ form an ASIC-POVM. \square

2.4 Construction II: Perturbing MUBs

We now describe a second, different, method to obtain a set of n^2 vectors such that the corresponding projectors span the space of all $n \times n$ matrices. This construction of ASIC-POVMs works for all dimensions n such that n is an odd prime number.

We note that all arithmetic operations in any expression involving elements of \mathbb{F}_p and real numbers are performed over the real numbers (where each element of \mathbb{F}_p is represented by an integer in the range $[0, p-1]$). For example, for a real $r \in \mathbb{R}$ and $a, x \in \mathbb{F}_p$, the power r^{ax} means r^u , where the integer $u = ax$ can be of size $(p-1)^2$.

Theorem 6. Let p be an odd prime number, and let $0 < r < 1$ be a real number. For $a, b \in \mathbb{F}_p$ define

$$|\varphi_{a,b}\rangle = \sqrt{\frac{1-r^{2a}}{1-r^{2pa}}} (r^{ax} \mathbf{e}_p(ax^2 + bx))_{x \in \mathbb{F}_p} \in \mathbb{C}^p.$$

and let $E_{a,b} = |\varphi_{a,b}\rangle \langle \varphi_{a,b}| / p$. Then the $E_{a,b}$ are linearly independent. Furthermore, let

$$G = \sum_{a,b \in \mathbb{F}_p} E_{a,b}.$$

Then for $r = 1 - p^{-3}$ the set $\{F_{a,b} : a, b \in \mathbb{F}_p\}$, with $F_{a,b} = G^{-1/2} E_{a,b} G^{-1/2}$ is an ASIC-POVM.

Proof. First, we show that the matrices $E_{a,b}$ are linearly independent. Note that instead of considering the normalized vectors $|\varphi_{a,b}\rangle$ it is possible to consider the vectors $|\tilde{\varphi}_{a,b}\rangle = (r^{ax} \mathbf{e}_p(ax^2 + bx))_{x \in \mathbb{F}_p}$ and to show that the corresponding projectors $\tilde{E}_{a,b} = |\tilde{\varphi}_{a,b}\rangle \langle \tilde{\varphi}_{a,b}|$ are linearly independent.

We use the technique introduced in [15] to check whether the matrices $\tilde{E}_{a,b}$ are linearly independent. To each $n \times n$ matrix $\tilde{E}_{a,b}$ we associate a state $|\tilde{E}_{a,b}\rangle$ which is simply the row-wise concatenation of the entries of $\tilde{E}_{a,b}$ as a vector of length n^2 . Then the matrices $\tilde{E}_{a,b}$ are linearly independent if and only if the matrix $S = \frac{1}{p} \sum_{a,b \in \mathbb{F}_p} |\tilde{E}_{a,b}\rangle \langle \tilde{E}_{a,b}|$ has full rank. We obtain

$$\begin{aligned} pS &= \sum_{a,b \in \mathbb{F}_p} |\tilde{E}_{a,b}\rangle \langle \tilde{E}_{a,b}| \\ &= \sum_{\substack{a \in \mathbb{F}_p \\ x,y,u,v \in \mathbb{F}_p}} r^{a(x+y+u+v)} \mathbf{e}_p(a(x^2 - y^2 - u^2 + v^2)) \\ &\quad \times \sum_{b \in \mathbb{F}_p} \mathbf{e}_p(b(x - y - u + v)) |x, y\rangle \langle u, v| \\ &= p \sum_{\substack{a \in \mathbb{F}_p \\ x,y,u,v \in \mathbb{F}_p}} r^{a(x+y+u+v)} \mathbf{e}_p(a(x^2 - y^2 - u^2 + v^2)) \delta_{x-y, u-v} |x, y\rangle \langle u, v|. \end{aligned}$$

The rows of S are labeled by pairs (x, y) , with $x, y \in \mathbb{F}_p$, and the columns by pairs (u, v) , with $u, v \in \mathbb{F}_p$. We first note that S can be written as a block-diagonal matrix of p submatrices, each of size $p \times p$, if the rows and

columns of S are suitably rearranged. For $0 \leq i \leq (p-1)$, we define the sets $\mathcal{L}_i = \{(x, x+i) : x \in \mathbb{F}_p\}$ (we treat i as an element of \mathbb{F}_p so $x+i$ is computed in \mathbb{F}_p too). We now order the rows and columns according to the list $\mathcal{L} = \bigcup_{i=0}^{p-1} \mathcal{L}_i$. With respect to this basis we obtain that

$$S = A_0 \oplus A_1 \oplus \dots \oplus A_{p-1},$$

with $p \times p$ matrices

$$A_i = \left[\sum_{a \in \mathbb{F}_p} r^{a(x+y+u+v)} \mathbf{e}_p(a(x^2 - y^2 - u^2 + v^2)) \right]_{x, u \in \mathbb{F}_p}$$

where $y = x + i$ and $v = u + i$. Hence, we obtain that

$$A_i = \left[\sum_{a \in \mathbb{F}_p} r^{2a(x+u+i)} \mathbf{e}_p(2ai(u-x)) \right]_{x, u \in \mathbb{F}_p}$$

and have to show that this matrix is invertible for $0 \leq i \leq (p-1)$. In order to do so, we first observe that $x \mapsto x - i/2$ defines a permutation of the rows of any $p \times p$ matrix and that similarly $u \mapsto u - i/2$ defines a permutation of the columns (hereafter $i/2$ is computed in \mathbb{F}_p). Applying both the row and the column permutation to A_i we obtain the matrix

$$B_i = \left[\sum_{a \in \mathbb{F}_p} r^{2a(x+y)} \mathbf{e}_p(2ai(u-x)) \right]_{x, u \in \mathbb{F}_p}.$$

Note further that $x \mapsto x/2$ and $y \mapsto y/2$ induce permutations of the rows and columns of any $p \times p$ matrix. Applying this to B_i we obtain the matrix

$$\begin{aligned} C_i &= \left[\sum_{a \in \mathbb{F}_p} r^{a(u+x)} \mathbf{e}_p(ai(u-x)) \right]_{x, u \in \mathbb{F}_p} \\ &= \left[\sum_{a \in \mathbb{F}_p} (r^x \mathbf{e}_p(-ix))^a (r^u \mathbf{e}_p(iu))^a \right]_{x, u \in \mathbb{F}_p} \\ &= \left[(r \mathbf{e}_p(-i))^{xk} \right]_{x, k=0}^{p-1} \times \left[(r \mathbf{e}_p(i))^{\ell u} \right]_{\ell, u=0}^{p-1}. \end{aligned}$$

Since $|r \mathbf{e}_p(i)| = |r \mathbf{e}_p(-i)| = r$ and $0 < r < 1$, by the property of Vandermonde matrices [32] we conclude that C_i is invertible for all $i = 0, \dots, p-1$ which implies that the matrices B_i , A_i , and finally S are invertible. Arguing as in the proof of Theorem 5 we have established the informational completeness of the projectors corresponding to the normalized vectors $|\varphi_{a,b}\rangle$.

Next, for $r = 1 - p^{-3}$ we derive the bound

$$|\langle \varphi_{a,b} | \varphi_{c,d} \rangle| \leq \frac{1 + o(1)}{\sqrt{p}}, \quad (a, b) \neq (c, d). \quad (7)$$

We have

$$|\langle \varphi_{a,b} | \varphi_{c,d} \rangle| = \sqrt{\frac{1-r^{2a}}{1-r^{2pa}}} \sqrt{\frac{1-r^{2c}}{1-r^{2pc}}} \left| \sum_{x \in \mathbb{F}_p} r^{(a+c)x} \mathbf{e}_p(\alpha x^2 + \beta x) \right|, \quad (8)$$

where $\alpha = a - c$ and $\beta = c - d$.

We frequently use that $r^t = 1 + O(t/p^3)$ for any $t = O(p^3)$. In particular,

$$\begin{aligned} \sqrt{\frac{1-r^{2a}}{1-r^{2pa}}} \sqrt{\frac{1-r^{2c}}{1-r^{2pc}}} &= \left(\sum_{x \in \mathbb{F}_p} r^{2ax} \right)^{-1/2} \left(\sum_{x \in \mathbb{F}_p} r^{2cx} \right)^{-1/2} \\ &\leq \left(\sum_{x \in \mathbb{F}_p} r^{2px} \right)^{-1} = (p(1 + O(1/p)))^{-1} \\ &= (1 + o(1))p^{-1}. \end{aligned}$$

Furthermore,

$$\begin{aligned} \left| \sum_{x \in \mathbb{F}_p} r^{(a+c)x} \mathbf{e}_p(\alpha x^2 + \beta x) \right| &\leq \left| \sum_{x \in \mathbb{F}_p} (1 + O(1/p)) \mathbf{e}_p(\alpha x^2 + \beta x) \right| \\ &\leq \left| \sum_{x \in \mathbb{F}_p} \mathbf{e}_p(\alpha x^2 + \beta x) \right| + O(1) \leq \sqrt{p} + O(1). \end{aligned}$$

Substituting the above bounds in (8), we derive (7).

Next, we note have that $E_{a,b} = |\varphi_{a,b}\rangle \langle \varphi_{a,b}| / p$ and $G = \sum_{a,b \in \mathbb{F}_p} E_{a,b}$. We now compute the frame operator G and show that G^{-1} is close to the identity.

Similarly to the proof of Theorem 5 this implies that $F_{a,b} = G^{-1/2}E_{a,b}G^{-1/2}$ indeed forms an ASIC-POVM. We have

$$\begin{aligned}
G &= \left(\sum_{\substack{a,b \in \mathbb{F}_p \\ x,y \in \mathbb{F}_p}} \frac{1 - r^{2a}}{p(1 - r^{2pa})} r^{a(x+y)} \mathbf{e}_p(a(x^2 - y^2) + b(x - y)) |x\rangle \langle y| \right) \\
&= \left(\sum_{\substack{a \in \mathbb{F}_p \\ x,y \in \mathbb{F}_p}} \frac{1 - r^{2a}}{1 - r^{2pa}} r^{a(x+y)} \mathbf{e}_p(a(x^2 - y^2)) \delta_{x,y} |x\rangle \langle y| \right) \\
&= \text{diag} \left(\sum_{a \in \mathbb{F}_p} \frac{1 - r^{2a}}{1 - r^{2pa}} r^{2ax} : x \in \mathbb{F}_p \right).
\end{aligned}$$

Recalling that $r = 1 - p^{-3}$, from the Taylor expansion we obtain that

$$\frac{1 - r^{2a}}{1 - r^{2pa}} = \frac{1 + o(1)}{p}.$$

Hence

$$\sum_{a \in \mathbb{F}_p} \frac{1 - r^{2a}}{1 - r^{2pa}} r^{2ax} = \frac{1 + o(1)}{p} \sum_{a \in \mathbb{F}_p} r^{2ax} = \frac{1 + o(1)}{p} (p + O(1)) = 1 + o(1).$$

Finally, we deduce that

$$\begin{aligned}
p^2 \text{tr}(F_{a,b} F_{c,d}) &= |\langle \tilde{\varphi}_{a,b} | \tilde{\varphi}_{c,d} \rangle|^2 = |\langle \varphi_{a,b} | G^{-1} | \varphi_{c,d} \rangle|^2 \\
&= (1 + o(1)) |\langle \varphi_{a,b} | \varphi_{c,d} \rangle|^2 = \frac{1 + o(1)}{p},
\end{aligned}$$

which implies that the rank one operators $F_{a,b}$ form an ASIC-POVM. \square

3 Relaxed MUBs and SIC-POVMs

3.1 Motivation

The constructions in the previous sections required the existence of $n + 1$ mutually unbiased bases in \mathbb{C}^n . Currently, it is not known whether such

extremal sets of mutually unbiased bases exist when n is divisible by two distinct primes. We show that approximately mutually unbiased bases exist in all dimensions. Furthermore, we show that if we slightly relax the ASIC-POVM condition, then we can obtain in any dimension systems of vectors that approximate SIC-POVMs. For these constructions, we need some results about the distribution of primes and bounds on exponential sums, which we summarize below.

These constructions work in any dimension n but attain its maximal strength for n of a certain arithmetic structure. In particular, if $n = p - 1$ for a prime p , then we show the existence of AMUBs in \mathbb{C}^n . It is not known whether maximal sets of MUBs in these dimensions exist.

Besides the general mathematical interest in the vector systems derived in this section, we expect that our approach and the new technique introduced in the following will lend themselves to some further applications in quantum information processing.

3.2 Analytic Number Theory Background

First of all we recall a remarkable result of [3] on gaps between consecutive primes.

Lemma 7. *For any sufficiently large x , any interval of the form $[x - x^{0.525}, x]$ contains a prime number.*

We now need some bounds of exponential sums with polynomials.

Let p be a prime number and let \mathbb{F}_p be a field of p elements. We always assume that \mathbb{F}_p is represented by the elements $\{0, \dots, p - 1\}$.

The following statement is a variant of the celebrated *Weil bound*, see Example 12 of Appendix 5 of [46] as well as Theorem 3 of Chapter 6 in [30] and Theorem 5.41 and comments to Chapter 5 of [31]).

Lemma 8. *Let χ be a nontrivial multiplicative character of \mathbb{F}_p of order s . Suppose that $G(X) \in \mathbb{F}_p[X]$ is not, up to a nonzero multiplicative constant, an s th power in $\mathbb{F}_p[X]$. Then for any polynomial $F(X) \in \mathbb{F}_p[X]$ of degree d we have*

$$\left| \sum_{u=1}^p \mathbf{e}_p(F(u)) \chi(G(u)) \right| \leq (d + \nu - 1)p^{1/2},$$

where ν is the number of distinct roots of G in the algebraic closure of \mathbb{F}_p .

We now use Lemma 8 to estimate some mixed exponential sums with two exponential functions.

Lemma 9. *Let $F(X) \in \mathbb{F}_p[X]$ be of degree $d \geq 2$. Then, for any integer k ,*

$$\left| \sum_{u=1}^p \mathbf{e}_p(F(u)) \mathbf{e}_n(ku) \right| = \begin{cases} O(p^{2/3}), & \text{if } d = 2, \\ O(p^{3/4}), & \text{if } d \geq 3. \end{cases}$$

Proof. Because each term in our sum is of absolute value $|\mathbf{e}_p(F(u)) \mathbf{e}_n(ku)| = 1$, for every integer $v \geq 0$ we have:

$$\sum_{u=1}^p \mathbf{e}_p(F(u)) \mathbf{e}_n(ku) = \sum_{u=1}^p \mathbf{e}_p(F(u+v)) \mathbf{e}_n(k(u+v)) + O(v).$$

Thus for every positive integer m we have

$$m \sum_{u=1}^p \mathbf{e}_p(F(u)) \mathbf{e}_n(ku) = \sum_{v=0}^{m-1} \sum_{u=1}^p \mathbf{e}_p(F(u+v)) \mathbf{e}_n(k(u+v)) + O(m^2).$$

Therefore

$$\left| \sum_{u=1}^p \mathbf{e}_p(F(u)) \mathbf{e}_n(ku) \right| \leq \frac{1}{m} W + O(m), \quad (9)$$

where

$$\begin{aligned} W &= \left| \sum_{u=1}^p \sum_{v=0}^{m-1} \mathbf{e}_p(F(u+v)) \mathbf{e}_n(k(u+v)) \right| \\ &= \left| \sum_{u=1}^p \mathbf{e}_n(ku) \sum_{v=0}^{m-1} \mathbf{e}_p(F(u+v)) \mathbf{e}_n(kv) \right| \\ &\leq \sum_{u=1}^p \left| \sum_{v=0}^{m-1} \mathbf{e}_p(F(u+v)) \mathbf{e}_n(kv) \right|. \end{aligned}$$

By the Cauchy inequality we obtain

$$\begin{aligned} W^2 &\leq p \sum_{u=1}^p \left| \sum_{v=0}^{m-1} \mathbf{e}_p(F(u+v)) \mathbf{e}_n(kv) \right|^2 \\ &= p \sum_{v,w=0}^{m-1} \mathbf{e}_n(k(v-w)) \sum_{u=1}^p \mathbf{e}_p(F(u+v) - F(u+w)). \end{aligned}$$

We now examine the polynomial $F_{v,w}(U) = F(U + v) - F(U + w)$. By the Taylor formula we have,

$$F_{v,w}(U) = F(U + v) - F(U + w) = \sum_{\nu=0}^{d-1} \frac{F^{(\nu)}(v) - F^{(\nu)}(w)}{\nu!} U^\nu.$$

Clearly $F^{(d-1)}(v) = F^{(d-1)}(w)$ is possible only for $v = w$. For such m pairs of v and w we estimate the sum over u trivially as p . Otherwise we estimate these sums as $(d-2)p^{1/2}$ by Lemma 8, getting

$$W^2 = \begin{cases} O(mp^2), & \text{if } d = 2, \\ O(mp^2 + m^2p^{3/2}), & \text{if } d \geq 3. \end{cases}$$

Thus by (9)

$$\left| \sum_{u=1}^p \mathbf{e}_p(F(u)) \mathbf{e}_n(ku) \right| = \begin{cases} O(m^{-1/2}p + m), & \text{if } d = 2, \\ O(m^{-1/2}p + p^{3/4} + m), & \text{if } d \geq 3. \end{cases}$$

Taking $m = \lceil p^{2/3} \rceil$ we conclude the proof. \square

We also need a special case of the classical *Weyl bound* which we present in the following form, see Lemma 3.6 of [25] or Lemma 2.4 of [43] for a similar statement in full generality.

Lemma 10. *Let $F(X) \in \mathbb{F}_p[X]$ be of degree $d \geq 2$. Then for any fixed $\varepsilon > 0$ and any integer $h \leq p$,*

$$\left| \sum_{u=1}^h \mathbf{e}_p(F(u)) \right| = O \left(h^{1+\varepsilon} \left(\frac{1}{h} + \frac{1}{p} + \frac{p}{h^d} \right)^{1/2^{d-1}} \right).$$

3.3 Arbitrary Dimensions

We now describe a construction of a vector system, which satisfies (4) exactly and also gives a certain approximation to (5). In fact we are able to get $n^d + 1$ (rather than $n + 1$) orthogonal bases with this property, where $d \geq 1$ is any integer.

Let \mathcal{F}_d be the set of polynomials of the form

$$f(X) = \sum_{\nu=2}^{d+1} a_\nu X^\nu.$$

with integer coefficients in the range $0 \leq a_\nu \leq n-1$, $\nu = 2, \dots, d+1$. Thus $\#\mathcal{F}_d = n^d$. Let p be the smallest prime with $p \geq n$. For each $f \in \mathcal{F}_d$ we consider the basis

$$\mathcal{B}_f = \{|\psi_{f,1}\rangle, \dots, |\psi_{f,n}\rangle\} \quad \text{where} \quad |\psi_{f,i}\rangle = \frac{1}{\sqrt{n}} (\mathbf{e}_p(f(u)) \mathbf{e}_n(iu))_{u=1}^n. \quad (10)$$

Theorem 11. *For any integer $d \geq 1$, the standard basis and the n^d bases \mathcal{B}_f , $f \in \mathcal{F}_d$, given by (10) are orthonormal and satisfy also*

$$\langle \psi_{g,j} | \psi_{f,i} \rangle = \begin{cases} O(n^{-1/3}), & \text{if } d = 1, \\ O(n^{-1/4}), & \text{if } d \geq 2, \end{cases}$$

where $f, g \in \mathcal{F}_d \cup \{0\}$, $f \neq g$, $1 \leq i, j \leq n$.

Proof. The orthonormality of each basis follows from the identity

$$\langle \psi_{f,j} | \psi_{f,i} \rangle = \frac{1}{n} \sum_{u=1}^n \mathbf{e}_n((i-j)u) = \delta_{i,j}.$$

Clearly, if $f \in \mathcal{F}_d$ and $g = 0$ (or $f = 0$ and $g \in \mathcal{F}_d$) then $|\langle \psi_{g,j} | \psi_{f,i} \rangle| = n^{-1/2}$. Thus it remains to estimate

$$\langle \psi_{g,j} | \psi_{f,i} \rangle = \frac{1}{n} \sum_{u=1}^n \mathbf{e}_p(f(u) - g(u)) \mathbf{e}_n((i-j)u)$$

for $f, g \in \mathcal{F}_d$, $f \neq g$ and $1 \leq i, j \leq n$.

Because

$$|\mathbf{e}_n(f(u) - g(u) + (i-j)u)| = 1$$

and by Lemma 7 we have

$$\begin{aligned} & \frac{1}{n} \sum_{u=1}^n \mathbf{e}_p(f(u) - g(u)) \mathbf{e}_n((i-j)u) \\ &= \frac{1}{n} \sum_{u=1}^p \mathbf{e}_p(f(u) - g(u)) \mathbf{e}_n((i-j)u) + O(|p-n|) \\ &= \frac{1}{n} \sum_{u=1}^p \mathbf{e}_p(f(u) - g(u)) \mathbf{e}_n((i-j)u) + O(n^{-0.475}). \end{aligned}$$

Hence,

$$\langle \psi_{g,j} | \psi_{f,i} \rangle = \frac{1}{n} \sum_{u=1}^p \mathbf{e}_p(f(u) - g(u)) \mathbf{e}_n((i-j)u) + O(n^{-0.475}).$$

Because $f(X) - g(X)$ is a polynomial of degree at least 2, Lemma 9 yields

$$\sum_{u=1}^p \mathbf{e}_p(f(u) - g(u)) \mathbf{e}_n((i-j)u) = \begin{cases} O(p^{2/3}) = O(n^{2/3}), & d = 1, \\ O(p^{3/4}) = O(n^{3/4}), & d \geq 2, \end{cases}$$

which concludes the proof. \square

As before, let p be the smallest prime with $p \geq n$. We consider n^2 vectors

$$\mathcal{B} = \{|\psi_f\rangle : f \in \mathcal{F}_2\}, \quad \text{where} \quad |\psi_f\rangle = \frac{1}{\sqrt{n}} (\mathbf{e}_p(f(u)))_{u=1}^n. \quad (11)$$

Theorem 12. *Let p be the smallest prime with $p \geq n$. Then, the vector system \mathcal{B} of n^2 vectors given by (11) is normalized and also satisfies*

$$|\langle \psi_g | \psi_f \rangle| \leq (2 + O(n^{-1/10})) n^{-1/2},$$

where $f, g \in \mathcal{F}_2$, $f \neq g$.

Proof. Obviously, we have

$$|\langle \psi_f | \psi_f \rangle| = 1, \quad f \in \mathcal{F}_2.$$

Put $h = p - n$. Then for $f, g \in \mathcal{F}_2$, $f \neq g$, we have

$$\begin{aligned} |\langle \psi_g | \psi_f \rangle| &= \frac{1}{n} \left| \sum_{u=1}^n \mathbf{e}_p(f(u) - g(u)) \right| \\ &= \frac{1}{n} \left| \sum_{u=1}^p \mathbf{e}_p(f(u) - g(u)) \right| + \frac{1}{n} \left| \sum_{u=1}^h \mathbf{e}_p(f(n+u) - g(n+u)) \right|. \end{aligned}$$

By Lemmas 8 and 10 we have

$$\begin{aligned} |\langle \psi_g | \psi_f \rangle| &\leq 2p^{1/2}n^{-1} + O\left(h^{1+\varepsilon}n^{-1} \left(\frac{1}{h} + \frac{1}{p} + \frac{p}{h^3}\right)^{1/4}\right) \\ &= 2p^{1/2}n^{-1} + O\left(n^{-1} (h^{3/4+\varepsilon} + h^{1+\varepsilon}p^{-1/4} + h^{1/4+\varepsilon}p^{1/4})\right). \end{aligned}$$

By Lemma 7 we see that $h = O(p^{0.525})$, therefore

$$h^{3/4+\varepsilon} + h^{1+\varepsilon}p^{-1/4} + h^{1/4+\varepsilon}p^{1/4} = O(p^{2/5}) = O(n^{2/5})$$

for sufficiently small ε and sufficiently large p . Noting that

$$p^{1/2} = (n + O(n^{0.525}))^{1/2} = n^{1/2} (1 + O(n^{-0.475}))^{1/2} = n^{1/2} + O(n^{0.2625})$$

we finish the proof. \square

3.4 Special Dimensions

Here we give some improvements of the constructions of Section 3.3 for the values of n for which the smallest prime p with $p \equiv 1 \pmod{n}$ is sufficiently small.

Let p be the smallest prime such that $p \equiv 1 \pmod{n}$. Let \mathcal{X}_n be the set of n characters of order n modulo p and \mathcal{U}_n the subgroup of residues of order n in \mathbb{F}_p^\times . In particular $\#\mathcal{U}_n = n$. It is known that \mathcal{X}_n is a cyclic group, so for some character $\chi \in \mathcal{X}_n$ all other characters of \mathcal{X}_n are given by the powers χ^i , $i = 1, \dots, n$.

For $f \in \mathbb{F}_p[X]$ of degree at most d and the above character $\chi \in \mathcal{X}_n$ we define

$$\mathcal{B}_f = \{|\psi_{f,1}\rangle, \dots, |\psi_{f,n}\rangle\} \quad \text{where} \quad |\psi_{f,i}\rangle = \frac{1}{\sqrt{n}} (\mathbf{e}_p(f(u))\chi(u)^i)_{u \in \mathcal{U}_n}. \quad (12)$$

Let \mathcal{G}_d be the set of polynomials of the form

$$f(X) = \sum_{\nu=1}^d a_\nu X^\nu.$$

with integer coefficients in the range $0 \leq a_\nu \leq n-1$, $\nu = 2, \dots, d+1$.

Theorem 13. *For any integer $d \geq 1$, the standard basis and the n^d bases \mathcal{B}_f , $f \in \mathcal{G}_d$, given by (12) are orthonormal and satisfy also*

$$|\langle \psi_{g,j} | \psi_{f,i} \rangle| \leq dp^{1/2}n^{-1},$$

where $f, g \in \mathcal{F}_d \cup \{0\}$, $f \neq g$, $1 \leq i, j \leq n$.

Proof. We have,

$$\langle \psi_{f,j} | \psi_{f,i} \rangle = \frac{1}{n} \sum_{u \in \mathcal{U}_n} \chi(u)^{i-j} = \begin{cases} 1, & i = j, \\ 0, & i \neq j, \end{cases} \quad 1 \leq i, j \leq n.$$

We also have

$$\begin{aligned} \langle \psi_{g,j} | \psi_{f,i} \rangle &= \frac{1}{n} \sum_{u \in \mathcal{U}_n} \mathbf{e}_p(f(u) - g(u)) \chi(u)^{i-j} \\ &= \frac{1}{p-1} \sum_{x=0}^{p-1} \mathbf{e}_p(f(x^{(p-1)/n}) - g(x^{(p-1)/n})) \chi(x^{(p-1)/n})^{i-j}. \end{aligned}$$

Now, using Lemma 8, we conclude the proof. \square

Corollary 14. *Let p be a prime and let $n = p - 1$. Then an AMUB exists in dimension n .*

Proof. We apply Theorem 13 for $p = n + 1$ and for $d = 1$. Hence, we have $n^2 + 1$ orthonormal bases such that inner products between their components are all bounded by $(n + 1)^{1/2} n^{-1} = n^{-1/2} + O(n^{-1})$. \square

4 Remarks and Open Questions

The questions about finding SIC-POVMs and MUBs can be reformulated as a spherical design question in the vector space \mathbb{C}^n (see Zauner's thesis [50] and also [28, 41]). Thus it is possible that the techniques of [29], as well as of more recent works, see a very inspiring survey [35], may apply to the problem of constructing systems of n^2 equiangular lines in \mathbb{C}^n , that is, SIC-POVMs. In fact, it is quite possible that with some adjustments they may also apply to MUBs.

It is widely believed, see [44], but remains unproved, that the smallest prime $p \equiv 1 \pmod{n}$ satisfies the bound

$$p = O(n \log^2 n).$$

In this case, the bound of Theorem 13 becomes $O(n^{-1/2} \log n)$. Thus, it is quite possible that the construction of Section 3.4 is always superior to those of Section 3.3.

Finally, we remark that many of the results of this paper remain unchanged if one uses prime powers $q = p^r$ (and thus general finite fields \mathbb{F}_q) instead of just primes p . In particular, Corollary 14 holds true in this more general setting. Hence, in summary, we have shown that ASIC-POVMs and AMUBs exist for any prime power dimension q . Moreover, we have shown that approximate versions of mutually unbiased bases and SIC-POVMs exist in any dimension if we are slightly more liberal about our constraints on the angles.

Acknowledgements

During the preparation of this paper, A. K. was supported in part by NSF CAREER award CCF 0347310, NSF grant CCR 0218582, a Texas A&M TITF initiative, and a TEES Select Young Faculty award, M. R. was at the Institute for Quantum Computing, University of Waterloo, where he was supported in part by MITACS and the *IQC Quantum Algorithm Project* funded by ARO/ARDA, I. S. was supported in part by ARC grant DP0211459, A. W. was supported in part by the Austrian Academy of Sciences and by FWF grant S8313.

This work was partially done during visits by I.S. to the Institute for Quantum Computing (Waterloo, Canada) and to the Johann Radon Institute for Computational and Applied Mathematics (Linz, Austria); the support and hospitality of these institutions are gratefully acknowledged.

References

- [1] D. M. Appleby. SIC-POVMs and the extended Clifford group. ArXiv preprint quant-ph/0412001, 2004.
- [2] M. Aschbacher, A. M. Childs, and P. Wocjan. The limitations of nice mutually unbiased bases. ArXiv preprint quant-ph/0412066, 2004.
- [3] R. C. Baker, G. Harman, and J. Pintz. The difference between consecutive primes, II. *Proc. Lond. Math. Soc.*, 83(3):532–562, 2001.

- [4] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34:512–528, 2001.
- [5] J. J. Benedetto and M. Fickus. Finite normalized tight frames. *Advances in Computational Mathematics*, 18(2–4):357–385, 2003.
- [6] I. Bengtsson and A. Ericsson. Mutually unbiased bases and the complementarity polytope. ArXiv preprint quant-ph/0410120, 2004.
- [7] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. of the IEEE Intl. Conf. Computers, Systems, and Signal Processing*, pages 175–179. IEEE, 1984.
- [8] J.-C. Boileau, J. Tamaki, K. Batuwantudawe, R. Laflamme, and J M. Renes. Unconditional security of three state quantum key distribution protocols. *Phys. Rev. Lett.*, 94:040503, 2005. See also ArXiv preprint quant-ph/0408085.
- [9] P. G. Casazza and J. Kovacevic. Equal-norm tight frames with erasures. *Advances in Computational Mathematics*, 18(2–4):387–430, 2003.
- [10] P.G. Casazza. The art of frame theory. *Taiwanese J. Math.*, 4(2):129–201, 2000.
- [11] C. M. Caves, C. A. Fuchs, and R. Schack. Quantum probabilities as Bayesian probabilities. *Phys. Rev. A*, 65:022305, 2002.
- [12] C. M. Caves, C. A. Fuchs, and R. Schack. Unknown quantum states: the quantum de Finetti representation. *J. Math. Phys*, 43(9):4537–4559, 2004.
- [13] S. Chaturvedi. Aspects of mutually unbiased bases in odd-prime-power dimensions. *Phys. Rev. A*, 65:044301, 2002.
- [14] M. Christandl, R. Renner, and A. Ekert. A generic security proof for quantum key distribution. ArXiv preprint quant-ph/0402131, 2004.
- [15] G. M. D’Ariano, P. Perinotti, and M. F. Sacchi. Informationally complete measurements and groups representation. *J. Opt. B: Quantum Semiclass. Opt.*, 6:S487–S491, 2004. See also ArXiv preprint quant-ph/0310013.

- [16] I. Daubechies. *Ten lectures on wavelets*. CBMS-NSF Reg. Conf. Series in Applied Math. SIAM, 1992.
- [17] T. Durt. Bell states, mutually unbiased bases, and the mean king's problem. ArXiv preprint quant-ph/0401037, 2004.
- [18] C. A. Fuchs. On the quantumness of a Hilbert space. *Quantum Information and Computation*, 4(6–7):467–478, 2004.
- [19] C. A. Fuchs and M. Sasaki. Squeezing quantum information through a classical channel: measuring the ‘quantumness’ of a set of quantum states. *Quantum Information and Computation*, 3:377–404, 2003.
- [20] M. Grassl. On SIC-POVMs and MUBs in Dimension 6. In *Proceedings ERATO Conference on Quantum Information Science (EQIS 2004)*, Tokyo, pages 60–61, 2004. See also ArXiv preprint quant-ph/0406175.
- [21] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé. The Z_4 -linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Transactions on Information Theory*, 40(2):301–319, 1994.
- [22] A. Hayashi, M. Horibe, and T. Hashimoto. The king's problem with mutually unbiased bases and orthogonal latin squares. ArXiv preprint quant-ph/0502092, 2005.
- [23] S. G. Hoggar. t -designs in projective spaces. *Europ. J. Combinatorics*, 3:233–254, 1982.
- [24] S. G. Hoggar. 64 lines from a quaternionic polytope. *Geom. Dedic.*, 69:287–289, 1998.
- [25] L. K. Hua. *Additive theory of prime numbers*. Amer. Math. Soc., 1965.
- [26] I. D. Ivanovic. Geometrical description of quantal state determination. *Journal of Physics A*, 14(12):3241–3245, 1981.
- [27] A. Klappenecker and M. Rötteler. Constructions of mutually unbiased bases. In *Proceedings the 7th International Conference on Finite Fields and Applications, Toulouse*, volume 2948 of *Lecture Notes in Computer Science*, pages 137–144. Springer-Verlag, 2004.

- [28] A. Klappenecker and M. Rötteler. Mutually unbiased bases are complex projective 2-designs. ArXiv preprint quant-ph/0502031, 2005.
- [29] V. I. Levenstein. Bounds for packing in metric spaces and certain applications. *Probl. Kibernetiki*, 40:44–110, 1983. (in Russian).
- [30] W.-C. W. Li. *Number Theory with Applications*. World Scientific, Singapore, 1996.
- [31] R. Lidl and H. Niederreiter. *Finite fields*. Cambridge University Press, Cambridge, 2nd edition, 1997.
- [32] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.
- [33] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [34] A. Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academic Publishers, 1993.
- [35] F. Pfender and G. M. Ziegler. Kissing numbers, sphere packings, and some unexpected proofs. *Notices Amer. Math. Soc.*, 132:873–883, 2004.
- [36] A. O. Pittenger and M. H. Rubin. Mutually unbiased bases, generalized spin matrices and separability. ArXiv preprint quant-ph/0308142, 2003.
- [37] M. Planat, H. Rosu, S. Perrine, and M. Saniga. Finite algebraic geometrical structures underlying mutually unbiased quantum measurements. ArXiv preprint quant-ph/0409081, 2004.
- [38] E. Prugovecki. Information-theoretical aspects of quantum measurement. *Int. J. Theor. Phys.*, 16:321–331, 1977.
- [39] J. M. Renes. Equiangular spherical codes in quantum cryptography. ArXiv preprint quant-ph/0409043, 2004.
- [40] J. M. Renes. Spherical code key distribution protocols for qubits. *Phys. Rev. A*, 70:052314, 2004. See also ArXiv preprint quant-ph/0402135.
- [41] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves. Symmetric informationally complete quantum measurements. *J. Math. Phys.*, 45(6):2171–2180, 2004.

- [42] J. Schwinger. Unitary operator bases. *Proc. Nat. Acad. Sci. U.S.A.*, 46:570–579, 1960.
- [43] R. C. Vaughan. *The Hardy-Littlewood method*. Cambridge University Press, Cambridge, 1997.
- [44] S. S. Wagstaff. Greatest of the least primes in arithmetic progressions having a given modulus. *Math. Comp.*, 33:1073–1080, 1979.
- [45] A. Weil. *Sur les courbes algebriques et les varietes qui s'en deduisent*. Hermann, Paris, 1948.
- [46] A. Weil. *Basic Number Theory*. Springer-Verlag, New York, 1974.
- [47] H. Weyl. Über die Gleichverteilung von Zahlen mod Eins. *Math. Ann.*, 77:313–352, 1916.
- [48] P. Wocjan and T. Beth. New construction of mutually unbiased bases in square dimensions. ArXiv preprint quant-ph/0407081, 2004.
- [49] W. Wootters and B. Fields. Optimal state-determination by mutually unbiased measurements. *Ann. Physics*, 191(2):363–381, 1989.
- [50] G. Zauner. *Quantendesigns – Grundzüge einer nichtkommutativen Designtheorie (in German)*. PhD thesis, Universität Wien, 1999.